Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

Jimmy Graham

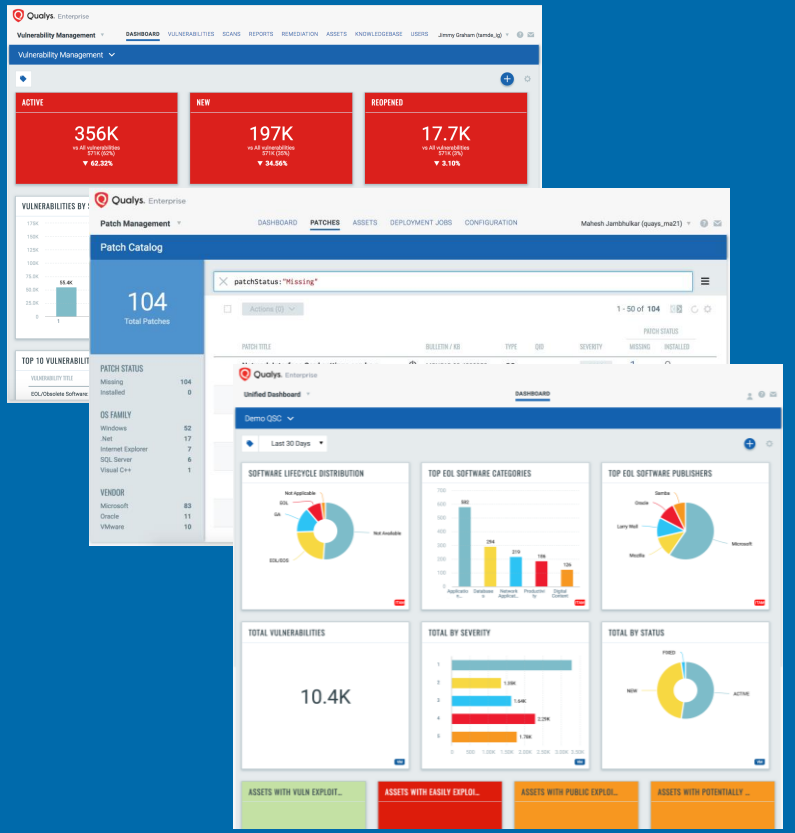
Senior Director, Product Management, Qualys, Inc.

Agenda

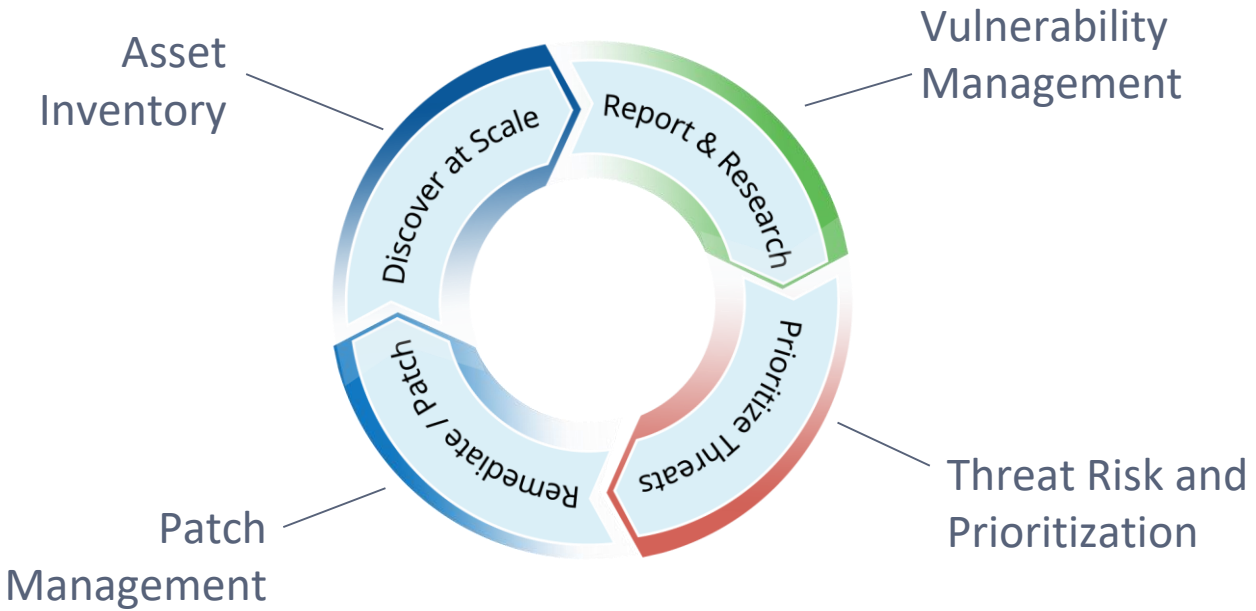
Expanding Vulnerability Management

Vulnerability Management Platform Evolution

Introducing Qualys Patch Management



Vulnerability Management Lifecycle



Expanding Vulnerability Management

Qualys.

Case Study: Large Bank

Challenge

Difficult to prioritize vulnerabilities across 100,000 endpoints

Manual correlation of external threat data

No active alerting on high-threat vulnerabilities

Low visibility into workstations

Solution

Threat Protection RTIs automates prioritization

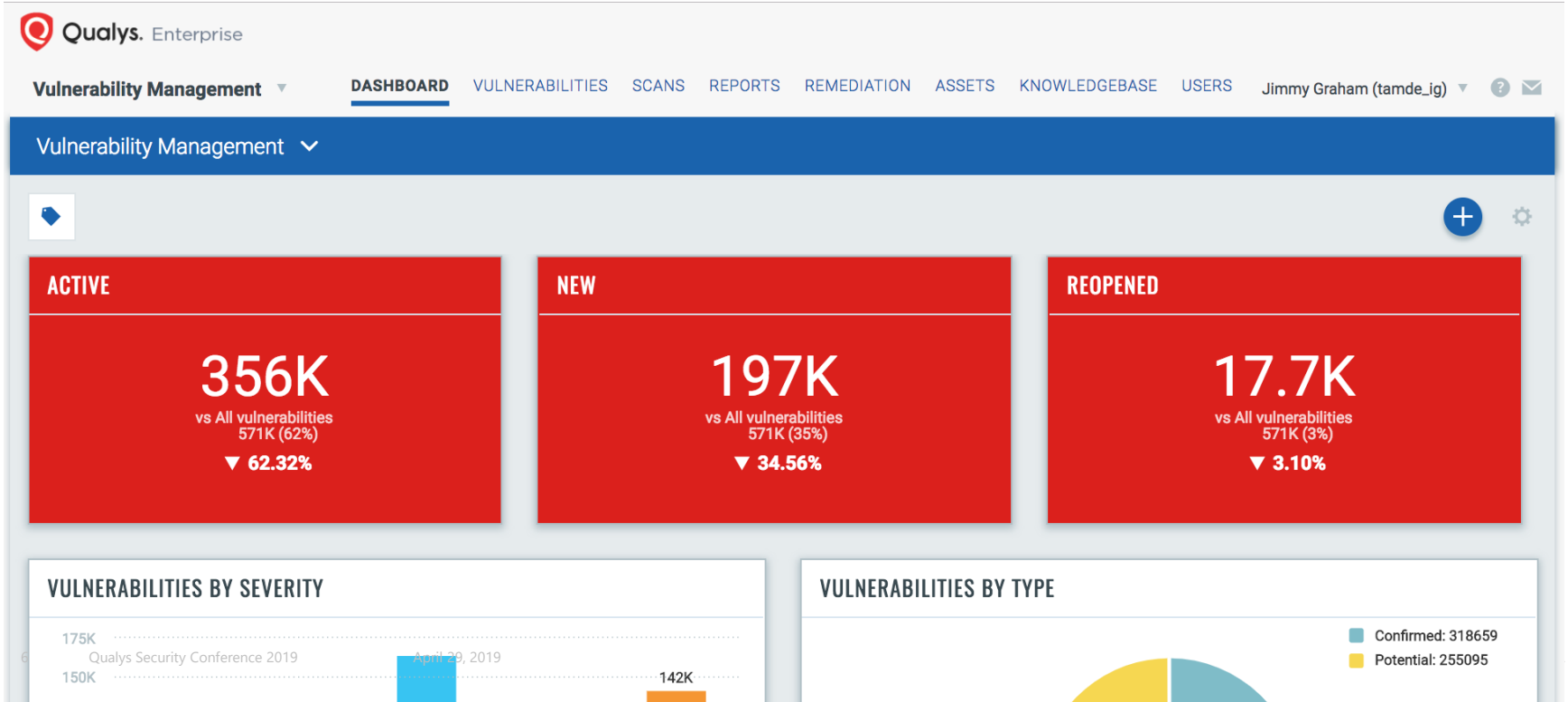
Threat Protection Live Feed provides one-click access to impacted assets

Continuous Monitoring combined with RTIs

Qualys Cloud Agent for continuous and complete visibility

Vulnerability Management

Platform Evolution



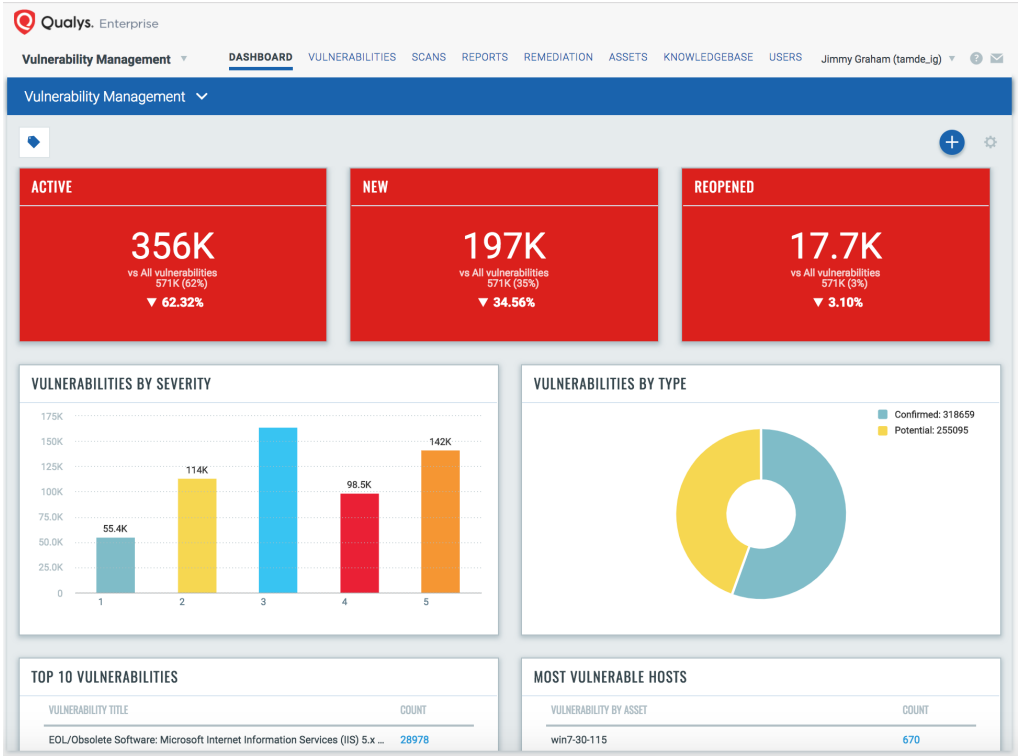
Dynamic VM Dashboard

Merges AssetView technology into Qualys VM

Build widgets with vulnerability counts

Search filters for quickly building queries

Replace long-running reports with live widgets



Qualys.

Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection Interface (QRDI)

Create your own or share on Qualys Community

Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic

Qualys.

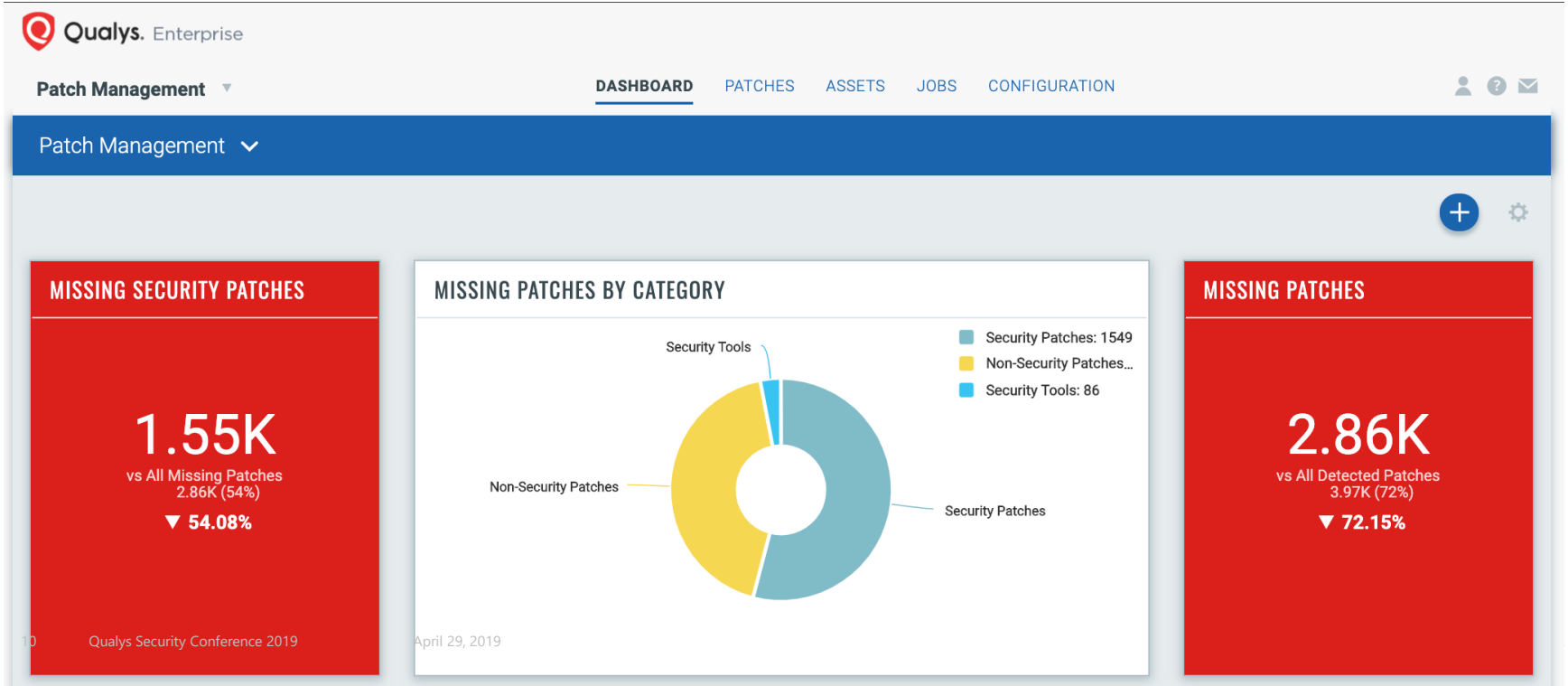
DEMO

Vulnerability Management

Dynamic Dashboard

Qualys Patch Management

Overview



Current Patch Management Tools

Challenges and Impact

Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation

Waiting for vulnerability reports to confirm remediation

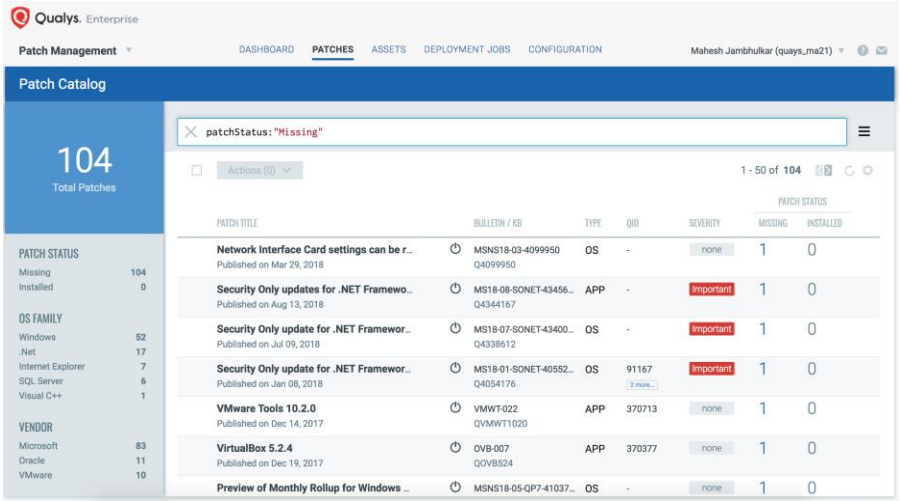
Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

Introducing

Qualys Patch Management



Automated correlation of vulnerability and patch data – Which patch fixes the CVE?

Simple dashboarding for tracking missing patches

Patch using the Qualys Cloud Agent, anywhere

Patch OS and third-party applications

Single solution for Windows, macOS, and Linux

Shift From Reaction Mode to Operational Security

Always up-to-date on missing patches

Security and IT teams can “speak the same language”

Collaboration – key to successful digital transformation

Unify discovery, prioritization, and remediation into one platform

Rapid remediation of high-profile vulnerabilities in days vs. weeks

Regularly scheduled deployments are repeatable and reported on

DEMO

Patch Management

Platform Support

XP SP3+
Vista
Windows 7
Windows 8/8.1
Windows 10
Server 2003 SP2+
Server 2008/R2
Server 2012/R2
Server 2016
Server 2019

OS X 10.10
Yosemite

OS X 10.11
El Capitan

macOS 10.12
Sierra

macOS 10.13
High Sierra

macOS 10.14
Mojave

RHEL 6,7

CentOS 5.4+,6,7

SUSE Linux Enterprise
Server/ Desktop
11,12,15

Oracle Ent Linux
6,7(Server)

Ubuntu
14.x,15.x,16.x,18.x

* Roadmap items are future-looking; timing and specifications may change

Qualys.

Patch Management Roadmap

Patch Management 1.0

March 2019

Windows patching (desktops and servers)

Qualys serves patches

Third party Windows applications

Patch Management 1.2

May 2019

On-prem Caching of patches (CAG)

Direct download from vendors for off-prem

Tag-based user scoping

Patch Management 1.3+

Mac patching

Linux patching w/

Repository integration

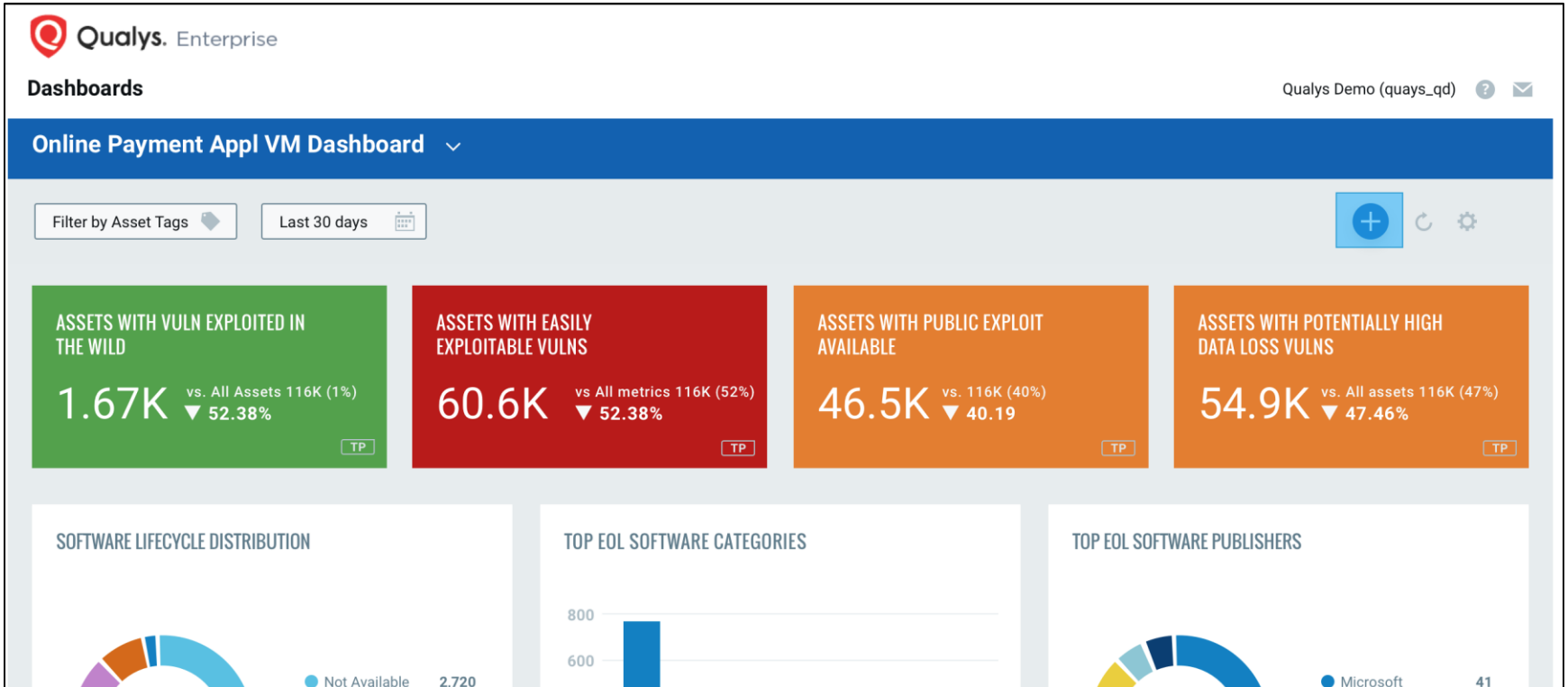
Role-based access control

Automation Rules & Approval workflows

Qualys.

Qualys Unified Dashboard

Preview



Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags

PREVIEW

Unified Dashboard

Unified Dashboard Rollout

Phase 1 – Q3 2019

Unified Dashboard App

Global dashboard filters

Support for:

VM PC FIM IOC

AI PM CRI TP

Phase 2 – Q1 2020

Unified widget builder

Upgrade existing Cloud App Dashboards

Support for:

WAS WAF SAQ

CS CV

Thank You

Jimmy Graham
jgraham@qualys.com